DERBYSHIRE
County Council

Information Security Document

Corporate Digital Records Preservation Policy

Version 10.0

Version History			
Version	**Date**	**Detail**	**Author**
1.0	28/09/2009	Approved by Information Governance Group	David Jenkins
2.0	27/07/2011	Reviewed by Information Governance Group	David Jenkins
3.0	31/10/2012	Reviewed by Information Governance Group	David Jenkins
4.0	29/11/2013	Reviewed by Information Governance Group. No changes.	David Jenkins
5.0	16/12/2014	Reviewed by Information Governance group. Updated with ISO27001:2013 controls.	David Jenkins
6.0	08/02/2016	Reviewed by Information Governance Group.	David Jenkins
7.0	06/03/2017	Reviewed by Information Governance Group. No changes.	David Jenkins
8.0	03/04/2018	Reviewed by Information Governance Group.	Mark Smith
9.0	07/05/2019	Reviewed by Information Governance Group. No changes.	Mark Smith
10.0	12/05/2020	Reviewed by Information Governance Group. Removal of floppy disks. Addition of services offered by the Record Office.	Mark Smith

This document has been prepared using the following ISO27001:2013 standard controls as reference:

ISO Control	Description
8.2.1>2	Classification of information
11.1.4	Protecting against external and environmental threats
8.3.1>2	Management of removable media
8.3.3	Physical media transfer
18.1.3	Protection of records

1. Introduction

1.1. The Code of Practice on Records Management issued by the Lord Chancellor under the Freedom of Information Act 2000 recommends public bodies across the country introduce a strategy for the preservation of digital records to ensure that they can continue to be accessed and used and are resilient to future changes in technology.

1.2. Many types of records and information that the Council uses have no paper counterpart and exist only in digital format. The preservation of digital records is complex and requires proactive intervention at various points within the lifetime of the record. ~~As digital records become the norm,~~ Addressing these issues is key to continued effective working by the Council, as well as to maintenance of the collective memory of its decision-making and service delivery.

1.3. Basic principles of records management and best practice in their application remain the same for digital as for paper records. Strategies and policies are in place for paper records. The purpose of this policy is to clarify their application to digital records.

1.4. It is the responsibility of Derbyshire County Council to have arrangements in place to enable the digital records it creates and uses to remain accessible.

1.5. Digital preservation is defined as “a series of managed activities necessary to ensure continued access to digital materials for as long as is necessary.” (Digital Preservation Coalition *Digital Preservation Handbook)*

1.6. Preservation arrangements can be divided into a number of phases:

1.6.1. Long Term: to allow continued access to digital materials, or the information they contain, indefinitely. Such arrangements should be in place for historically important records to be transferred in due course to Derbyshire Record Office

1.6.2. Medium Term: to allow access for a set period of time, irrespective of changes in technology. Time limits should reflect records retention periods in departmental records schedules

1.6.3. Short Term: to allow access to digital materials for a set period of time while needed for business, legal, financial or similar operational purposes

2. Aims and Objectives:

2.1. This policy aims to raise awareness of digital preservation as a major concern for the Council in how it creates and manages its digital records.

2.2. This policy, and associated procedures, will outline current best practice to mitigate risks in dealing with digital records.

3. Examples of digital records:

3.1. The following are the main types of digital records covered by this policy:

3.2. ‘Born-digital’ records including documents created using Microsoft Office applications (Word-Processed documents, spreadsheets, databases, emails etc) in addition to records kept in dedicated case management systems (including Mosaic).

3.3. Digital Surrogates created following scanning of paper documents. These are scanned image files of paper files created in order to improve workflow or to rationalise space.

4. Strategies to assist with digital preservation:

4.1. Maintaining access to digital records over a lengthy period of time requires a continuous cycle of actions in respect storage media, content, contextual information, and safeguarding from threats of software and technological obsolescence, malfunction and deterioration.

4.2. Digital records, like their paper equivalents, should be managed in accordance with an agreed records retention schedule. Disposal arrangements need to be in place. The General Data Protection Regulation, Environmental Information Regulations, Freedom of Information Act and Data Protection Act all apply equally to paper and electronic records.

4.3. In order to preserve a record, it must first be effectively managed. Following basic records management principles will help ensure, at an early stage, that digital records which merit permanent preservation are identified. By identifying these records, time and resources will be saved by making appropriate disposal arrangements for time-expired records.

4.4. When embarking upon a digitisation project, staff should seek to ensure that the most appropriate file-formats are used which will ensure long term preservation and accessibility. This decision should be made at the outset of any project. Derbyshire Record Office can advise on how to plan a digitisation project that will work within the framework of the Corporate Records Management Policy and the Corporate Scanning Policy.

4.5. Storage media for digital records have limited lifespans. ~~3.5'' floppy disks were commonly used from the 1990s to the early 2000s, today these are no longer supported by most major computer systems. CD-R compact-disks are recommended as the most resilient storage media.~~ Regular quality checks should be carried out to ensure the digital records held on storage media are intact and readable.

4.6. Owing to the short lifespan of electronic storage media, it may be necessary to migrate data from one storage media to another after a set period. Further guidance on migration procedures is available from Derbyshire Record Office.

4.7. Records created using open-source software are often easier to migrate than their proprietary counterparts.

4.8. In respect of digital images, TIFFs are regarded as the most appropriate file format for long term digital preservation .For access purposes JPEGs (or similar file formats of a smaller file size) should be used.

4.9. For other documents, the use of approved, established and reliable software is recommended.

4.10. Derbyshire Record Office accepts digital records as permanent records if they possess exceptional historical value, or if the retention schedule directs that they should be offered to the record office at the end of their lifecycle.

5. Roles and Responsibilities:

5.1. Departmental/Service/Section Heads:

Responsible for ensuring that:

5.1.1. The corporate digital preservation policy and its associated guidelines are implemented within their department/service/section.

5.1.2. Staff are supported in terms of training and development to enable them to address digital preservation issues.

5.1.3. Digital preservation considerations are taken into account when considering digitisation initiatives or procuring new software or hardware.

5.1.4. Where appropriate, strategies are put in place to ensure the regular migration of records held solely in digital format.

5.2. Derbyshire Record Office:
Responsible for ensuring that:

5.2.1. Appropriate advice and guidance is given to Members and Senior Officers.
5.2.2. Professional standards for digital preservation are met and that compliance is regularly reviewed.
5.2.3. Records identified for permanent preservation are transferred as appropriate to Derbyshire Record Office.
5.2.4. Periodic audits of records and information are undertaken across the Council to identify good practice and levels of compliance, the outcome of which should be reported to the Information Governance Group.

6. Policy Monitoring and Review:

6.1. Compliance with this policy and related guidelines will be monitored by the Archives and Local Studies Manager and Corporate Records Manager in consultation with departmental representatives
6.2. As part of monitoring and evaluation procedures, a digital preservation risk assessment and an action plan will be formulated and reviewed

7. Breaches of Policy

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to Council assets, or an event which is in breach of the Council’s security procedures and policies.
All Council employees, elected members, volunteers, partner agencies, contractors and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible through the Council’s Incident Reporting Procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of the Council.

The Council will take appropriate measures to remedy any breach of the policy and its associated procedures and guidelines through the relevant frameworks in place. Where it becomes apparent that there may have been a breach of this policy by an employee then the matter may be dealt with under the disciplinary process.

This document is owned by the Information Governance Group and forms part of the Council's ISMS Policy and as such, must be fully complied with.